Wexford County Council

Data Protection Policy

Data Protection Acts, 1988 to 2003 as amended.

November 2016, as adopted.

Wexford County Council.
Data Protection Policy.

Introduction:

Wexford County Council is the democratically elected unit of Local Government in County Wexford and is responsible for the provision of an extensive and diverse range of services to the people of the County.

From 1st July, 2014, under the provisions of the Local Government Reform Act, 2014, following the abolition of town councils Wexford County Council became the Data Control Authority for all local government activity in the County.

In performing its functions, the Council is required to collect and process significant amounts of "Personal Data" and "Sensitive Personal Data" within the meaning of the Data Protection Acts 1988 and 2003 (DPA).

These Acts provide that "Personal Data" and "Sensitive Personal Data" must be collected and used fairly, be stored safely and securely, and not disclosed to any third party unlawfully.

Data in this policy document means both personal data and sensitive personal data.

Wexford County Council is committed to protecting the rights and privacy of individuals in accordance with current Data Protection legislation.
In particular we are committed to protecting personal data as enshrined in the second title (Freedoms) of the Charter of Fundamental Rights of the European Union which has full legal effect under the Treaty of Lisbon since 1st December 2009.

This policy must be read in conjunction with the Data Protection Acts 1988 and 2003 (DPA) and Regulations made thereunder.

It sets out how the Council will handle and process data, deal with a request for data by a data subject and manage a breach of data.

It also references the controls in place in respect of the use of CCTV systems and requests for data images.

Data is collected for any one of the 150 plus services the Council provides to the citizens of County Wexford. It collects it on paper, by way of application forms, correspondence etc. It also receives data by way of emails and holds data electronically on shared drives and servers.

It all cases it must ensure that data is obtained for stated specified purposes consent for such data is obtained, that it is held securely and not held for longer than required.

Appendix 1 sets out the definitions for terms used in this policy document.

1. **Policy in Respect of Compliance with the Data Protection Acts.**

It is the policy of Wexford County Council to comply fully with the Data Protection Acts. It will, as a Data Control Authority, carry out all duties and functions as set out in the Acts and ensure that the gathering and holding of data is done so solely within the terms of the Acts.

2. **Appointment of a Data Controller.**

It is the policy of Wexford County Council to have a Data Controller. It has done so by appointing the County Secretary as Data Controller under Executive Order no. 150 / 2015 dated 6th May, 2015.

3. **Policy in Respect of Registration of Data.**

It is the policy of Wexford County Council to annually register the types and details of data it processes with the Data Protection Commissioners Office. This is a legislative requirement under Section 16 of the Act.
The Public Register can be viewed on the Commissioners website www.dataprotection.ie .
The Council's registration reference is 0275/A.

The Council registers information under the following headings on the Register annually:

A. A Description of both Personal Data and Sensitive Personal Data held by the Council.
B. A list of the persons or bodies to which this Data may be disclosed.
C. A list of the countries or territories to which the Council may transfer the Data.
D. Details of the types of Sensitive Data held by the Council.
E. The uses for which this Sensitive Data is put.
F. Details of the security safeguards in place to protect the privacy of Data held by the Council.

4. **Policy in Respect of Adherence with Guidelines issued by the Office of the Data Protection Commissioner.**

It is the policy of Wexford County Council to adhere to all guidelines issued by the Office of the Data Protection Commissioner.
These include guidance on such matters as CCTV, records management as well as rulings in respect of complaints made to that Office.

5. **Policy in Respect of Data Protection Rules.**

It is the policy of Wexford County Council to adhere to the following eight Data Protection rules which are fundamental to Data Protection law.

They outline the responsibilities of a Data Controller and its employees in processing both personal data and sensitive personal data. The rules also apply to persons acting as Data Processors on behalf of the Data Controller.

The Rules are to:

1. Obtain and process the information fairly.

2. Keep it only for one or more specified, explicit and lawful purposes.

3. Process it only in ways compatible with the purposes for which it was given to the Council initially.

4. Keep it safe and secure.

5. Keep it accurate and up-to-date.

6. Ensure that it is adequate, relevant and not excessive.

7. Retain it no longer than is necessary for the specified purpose or purposes.

8. Give a copy of his/her personal data to any individual, on request.

6. Policy in Respect of Rights of the Individual. (A Data Subject means an individual who is the subject of personal data.)

It is the policy of Wexford County Council to ensure that the rights of the Individual are fully protected as set out below and the Council will release information following a request in accordance with these rights:

Rights of individuals:

1. An individual has the right to find out if the Council holds data on them.

2. An individual has the right to know the description of any data held on them.

3. An individual has the right to know the purpose for holding such data.
   (Requests for nos. 1 to 3 above must be in writing and is free of charge.)

4. Right of Access.
   An individual has the right to get a copy of personal information held by a Data Controller about him.
   (This request must be submitted in the form of a written request known as an “Access Request”. There may be a fee of up to €6.35 for this information.)

5. An individual has the right of rectification, erasure and / or blocking if data is no longer relevant or inaccurate.

6. An individual has the right to have their name removed from a direct marketing list such as an edited version of the Electoral Register.

7. An individual has the right to complain to the Data Protection Commissioner if an access request is not responded to fully or partially within set time periods.

8. An individual has the right to seek compensation through the Courts for any harm or distress; e.g., if damage is suffered by an individual through mishandling of data.

7. Policy in Respect of Managing Data Protection Breaches.

It is the policy of Wexford County Council to manage breaches of data protection in accordance with the DPA, this policy document and guidelines as issued by the Office of the Data Protection Commissioner.

A data protection breach occurs where personal data or sensitive personal data is released without authority or consent. Such breaches may occur in the event of the loss of USB keys, disks, laptops, digital cameras and mobile phones, or other electronic devices on which data is held, as well as paper records containing data.

A breach may also occur due to inappropriate access to such data on Wexford County Council systems or the sending of data to the wrong individuals.

In the event of a Data Protection Breach measures will be put in place to prevent a repetition of the incident.

All affected individuals will be notified without delay and an investigation immediately commenced. The Data Protection Commissioners Office will be contacted, and where the numbers of persons affected exceed a certain limit, all will be notified as directed by that Office.

The findings of the investigation and recommendations will be advised to the Data Protection Commissioners Office and to affected individuals. All recommendations will be implemented as soon as possible.

8. Policy in Respect of Promoting Awareness of Data Protection among Staff and others who carry out Data Processing for the Council.

It is the policy of Wexford County Council to ensure compliance with the Data Protection Acts. It will ensure compliance with the legislation among its staff and any persons acting as Data Processors on its behalf.

All employees of the Council who collect and / or control the contents and use of personal data are also responsible for compliance with the DPA.

The Council will continue to provide support, assistance, advice and Data Protection Awareness training to staff to ensure compliance with the legislation.

9. Policy in Respect of a Records Management Policy to ensure the security and ready access of data.

It is the policy of Wexford County Council to implement a Records Management Policy throughout the organisation. These records contain information as well as data.

The Policy is designed to ensure that there is a standardised filing system in which data is securely held and is readily accessible and retrievable in the event of a subject access request and a Freedom of Information request.

In order to ensure a standardised filing methodology, guidance notes on the use of electronic drives, including usage of folder and sub-folder files and categorising and filing of emails will be developed and issued to staff.

Data and information can be held on the following:

- Paper records, application forms etc.,
- Electronic Files on Shared and stand alone drives,
- Emails,
- Diaries,
- Accounts,
- Registers,
- Note Books,
- Tapes,
- DVDs'
- Servers,
- CDs' etc.,
- Website., Intranet.
- Drawings, Maps etc.

The Records Management Policy will also be designed to enable the regular systematic deletion of records in line with the policy. In order to ensure full deletion all traces of the electronic footprint will have to be deleted as well as the corresponding paper file.

10. Policy in Respect of Developing a Data Protection Expertise.

It is the policy of Wexford County Council to train staff in Data Protection law and precedents in order to have that expertise available to advise on queries and subject access requests when received.

The Freedom of Information Office is the primary point of contact for the public wishing to make subject access requests as well as for contact by the Office of the Data Protection Commissioner.

11. Policy in Respect of Handling a Subject Access Request (SAR).

It is the policy of Wexford County Council to have a central point of access for D. P. requests as well as providing assistance to requesters. A Data Access Request must meet certain requirements as specified in the Data Protections Acts.

These are:

- It must be in writing.
- It must include a reasonable level of appropriate information to enable the Council to locate the information required.
- Wexford County Council will make reasonable enquiries to satisfy itself about the identity of the person making the request to ensure personal data is only released to those entitled to it..
- Varying time limits for Subject Access Requests apply, depending on the data sought, and the Council will endeavour to adhere to these. Where reasonable additional information is required to substantiate the request, the time frame for responding runs from receipt of the additional information.
- In the event of receiving a very general Data Access Request, e.g. “please give me everything you have on me”, the Data Protection Acts provides for the seeking of more detailed information on the nature of the request, such as the approximate date of a particular incident, our reference number, the identity of the other party, etc.
- Wexford County Council may charge the statutory fee of €6.35 before it will deal with a Data Access Request.

The policy and procedure in relation to requests by the Garda Síochána (or other law enforcement or investigation agency) for access to data from council records in relation to the prevention, detection or prosecution of offences or investigations of incidents is that any such request should:

- Be made in writing.
- Provide detail in relation to the data required.
- State the reason it is required.
- Quote the relevant legislation which applies to their request for data.
- Be signed by a person at management level in the organisation, e.g. Garda Sargeant in Charge, Investigating Manager etc.

12. Policy in Respect of Restriction on the rights of access:

It is the policy of Wexford County Council to examine each request to ensure that data which can be released is released and that restrictions on release under the Acts are adhered to.

The release of records and data is governed by the Data Protection Acts which also contains some restrictions to the full or partial release of data under Section 5 of the Acts. Some of these are:

1. For the purpose of preventing, detecting or investigating offences,
2. Apprehending or prosecuting offenders,
3. Assessing monies due to the State
4. Subject to legal professional privilege,
5. Kept only for statistical research and the results are not made available in a way that identifies data subjects.
6. Back – up data.

13. Policy in Respect of CCTV.

It is the policy of Wexford County Council to develop a policy in respect of CCTV systems operated by the Council in the County. The policy will distinguish between private and public CCTV and body worn equipment. It will provide for a 28 day deletion of images, restricted access to monitors, servers and recording equipment and security to ensure images are neither deleted or modified.

Requests for images can be made by the Garda Síochána, other enforcement or investigation agencies or the public, who must demonstrate a legitimate reason for a request. Images released must be pixilated to ensure the privacy of others captured on CCTV.

The policy will distinguish between private and public CCTV. As well as holding personal and sensitive data as set out above and the seeking of access to it, requests for CCTV images and recordings can be made by the Garda Síochána and others who can demonstrate a legitimate reason for the request.

Applications are made as follows:

- In writing.
- Provide detail in relation to the data required. In particular the time at which an incident may have taken place must be specified as extended viewing of captured images is not allowed under the DPA.
- State the reason it is required.
- Quote the relevant legislation which applies to their request for data.
- Be signed by a person at management level in the organisation, as applicable.

14. Policy in Respect of Data Controller in relation to Access Requests.

It is the policy of Wexford County Council that the Data Controller will make the final decision as to what should be released and will ensure that the content of data is fully protected, even if released by request.

This role extends to the examination of pixilated CCTV images and stills to ensure no images of persons not making a request are released.

15. Policy in respect of the Review of this Policy Document and New EU Data Protection Regulation.

It is the policy of Wexford County Council to review this policy periodically in light of its operation and in terms of new legislative or other relevant factors and following guidance from the Office of the Data Protection Commissioner.

The EU General Data Protection Regulation come into effect on 25th May, 2018 for all EU member states, including Ireland.

It will repeal and replace the DPA and Wexford County Council, as a Data Controller, must implement the Regulation from that date.

The main features of the Regulation are contained in Appendix 2 attached.

Appendix 1. **Definitions:**

The DPA contain numerous definitions, the main ones being outlined hereunder. In all cases reference will be made to the Acts.

Data: Means automated data and manual data. This includes computerised systems, paper based filing systems, photographs and CCTV images etc.

Data Controller: Is a person who, either alone or with others, controls the contents and use of personal data. They would collect, store and process data about a living person on any computerised or structured manual filing system.

Data Processor: Is a person who processes data on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of his employment. Outsourcing payroll services is an example of a Data Processor.

It is the responsibility of the Data Controller to ensure that the Data Processor handles the data within the provisions of the DPA.

Data Protection: Safeguarding of privacy rights of individuals in relation to processing of their personal data and sensitive personal data as provided for under the DPA.

Data Subject: Is an individual who is the subject of personal data.

Personal Data: Is Data relating to a living individual who is or can be identified either from the data or from in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

Processing: Processing of or in relation to information or data, means performing any operation or set of operations on the information or data, whether or not by automatic means, including—
obtaining, recording or keeping the information or data, collecting, organising, storing, altering or adapting the information or data, retrieving, consulting or using the information or data disclosing the information or data by transmitting, disseminating or otherwise making it available, or aligning, combining, blocking, erasing or destroying the information or data;",

Sensitive Personal Data: Is personal data as to the

- racial or
- ethnic origin,
- the political opinions or
- the religious or
- philosophical beliefs of the data subject,
- whether s/he is a member of a trade union,
- the physical or
- mental health or
- condition or
- sexual life of the data subject,
- the commission or alleged commission of any offence by her/him,
- any proceedings for an offence committed or alleged to have been committed by the data subject,
- the disposal of such proceedings or
- the sentence of any court in such proceedings.

Subject Access Request: A request made by an individual for personal / sensitive data held on him.

Appendix 2. The General Data Protection Regulation (GDPR).

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

The GDPR will come into effect on 25th May, 2018.

The main provisions are as follows:

Chapter I: General Provisions; Scope, Definitions.

Chapter II: Principles relating to the processing of data; Lawfulness, Consents etc.

Chapter III: Rights of the Data Subject; Access, Erasure, Rectification, Right to Object to Processing, Legislative right to States to restrict access for National Security etc. reasons.

Chapter IV: Data Controller and Processor; Roles Responsibilities, Data Protection Officer, Security of Personal Data, Handling of Data Breaches, Data Protection Impact Assessment, Codes of Conduct.

Chapter V: Transfers of personal data to third countries or international organisations

Chapter VI: Independent Supervisory Authorities.

Chapter VII: Cooperation between Lead and Supervisory Authorities, European Data Protection Board.

Chapter VIII: Rights to Remedies, Liability and Penalties.

Chapter IX: Specific processing Provisions; Freedom of Expression and Information, Access to Public Documents, Obligations of Secrecy etc.,

Chapter X: Delegated Acts and Implementing Acts.

Chapter XI: Final Provisions, Repeal of Previous Directives, Commission Review of Operations of GDPR, Effective Date ec.

The main provisions affecting Wexford County Council will be:

The appointment of a Data Protection Officer (DPO)

The Designing - in of data protection during development and roll-out of new services and technology.

The adoption of a Risk Impact Assessment and Breach Management Policy.

Strengthening of data security so as to avoid liability for the new fines mechanism for breaches of data protection and the mis-management of personal data. Greater encryption and other methods of protecting data must be provided.

The reporting of data breaches must be reported within 72 hours,

Systems to ensure that data of all records, paper, electronic and emails in terms of A right to be forgotten will require the permanent deletion of data.

ends.